UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/854,437	05/11/2001	Victor B. Lortz	42390.P10873	7249

7590 07/29/2005

Crystal D. Sayles
c/o BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
12400 Wilshire Boulevard
Seventh Floor
Los Angeles, CA 90025

EXAMINER	
ARANI, TAGHI T	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 07/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/854,437	LORTZ, VICTOR B.	
	Examiner	Art Unit	
	Taghi T. Arani	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 May 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *04 September 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-30 have been examined and are pending.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.1 14, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.1 14, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.1 14. Applicant's submission filed on 05/09/2005 has been entered.

Response to Arguments

3. Applicant's arguments filed 05/09/2005 with respect to claims 1-30 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. **Claims 1-4, 9, 11-14, 19-22, 24, 26 and 28-29** are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Pat. No. 6,209,101 to Mitchem et al. (hereinafter " Mitchem") and further in view of U.S. Pat. No. 6,067,623 to Blakely et al. (hereinafter "Blakely).

As per claims 1, Mitchem is directed to a method, Apparatus, system and computer executable instructions for controlling access to protected information resources (see abstract, Figure 1 and associated text, claims 26 and 27).

receiving a resource request from a first requestor (col. 3, lines 18-23, Figure 1, resource request 40 issues a resource request 50 to enforcement mechanism 20 when desiring to operate on one of the computing resources 25), the resource request including identifying information regarding an operation to be performed with respect to a resource (col. 3, lines 20-23, task 40, for example, may issue resource requests in order to mount a network drive, retrieve information or delete a particular file.);

mapping the resource request to a resource identifier (col. 3, lines 23-27, enforcement mechanism queries policy resolution by identifying requesting tasks 40, the requested resource 25 and the desired operation to be performed on the resource, i.e. mapping the resource request to a resource identifier);

searching a resource data structure for a resource node based on the resource identifier (col. 3, lines 44-45, policy resolution mechanism accesses a security database of the stored security association);

determining whether the first requestor is authorized to perform the operation with respect to the resource based on resource authorization parameter associated with the resource node (col. 3, lines 41-51, policy resolution mechanism 30 maintains the set of security associations as an access matrix having tasks 40 and resources 25 as indices and based on security association, policy resolution mechanism issues a response indicating whether the resource request is granted).

Mitchem does not disclose but Blakely discloses a resource request including credentials (see abstract, see also col. 4, lines 50-65, col. 5, lines 7-21), translating the resource request to a resource inquiry request (col. 4, lines 23-30, Id mapping), the resource inquiry request including a resource authorization parameter representing the permission necessary for a client to perform the operation (Id mapping is process of determining that client1 is mapped to ERID5 (resource authorization parameter representing the permission necessary for the client) and determining the resource request.authorization based on whether the credentials in the resource request match the resource authorization parameter associated with the resource node (col. 4, lines 31-41, credential transform, where the mapped Id (if properly authorized) is used to access necessary credentials and the original client request is modified to incorporate the transformed credentials to access to the resource).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the Id mapping and credentials transform of Blakely within the access controlling method, system and computer executable instructions of Mitchem with a motivation to enable tasks (clients) of Mitchem to access multiple separately authenticated resources with a single authentication (see Blakely, col. 1, lines 6-14).

As per claim 12, Mitchem teaches an apparatus comprising (Fig. 1 and associated text, security system 10):

a memory for storing a resource data structure having resource nodes each of

which represents a respective resource and which has a respective resource identifier and resource authorization parameter (col. 3, lines 39-44, policy resolution mechanism maintains the set of security associations as an access matrix having tasks 40 and resources 25 as indices and each entry of the access matrix defines a set of operations that the corresponding task 40 is permitted to invoke on a particular resource 25); and

a processor (Figure 1, policy resolution mechanism 30) configured to:

receive a resource request from a first requestor, the resource request including identifying information representing an operation to be performed with respect to a resource (col. 3, lines 23-27, enforcement mechanism 20 receives re resource request and identifies the requesting task 40, the requested resource 25 and the desired operation to be performed on the requested resource 25, col. 3, line 23-27);

map the resource request to a resource identifier (col. 3, lines 23-27, enforcement mechanism queries policy resolution by identifying requesting tasks 40, the requested resource 25 and the desired operation to be performed on the resource mapping the resource request to a resource identifier);

search the resource data structure for a resource node based on the resource identifier (col. 3, lines 44-45, policy resolution mechanism accesses a security database of the stored security association (i.e. searching the access matrix based on the resource identifier); and

determine whether the first requestor is authorized to perform the operation with respect to the resource based on the resource authorization parameter associated with the resource node (col. 3, lines 41-51, policy resolution mechanism 30

maintains the set of security associations as an access matrix having tasks 40 and resources 25 as indices and based on security association , policy resolution mechanism issues a response indicating whether the resource request is granted).

Mitchem does not disclose but Blakely discloses a resource request including credentials (Blakely, see abstract, see also col. 4, lines 50-65, col. 5, lines 7-21) and determining whether the first requestor is authorized to perform the operation with respect to the resource based on whether the credentials in the resource request match the resource authorization parameter associated with the resource node (Blakeley, col. 4, lines 18-41, Id mapping and credential transform of middle tier server maps and credential transforms a client id (client1) to a resource authorization parameter (ERID5) to access necessary credentials and the original client request is modified to incorporate the transformed credentials to access to the resource).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the Id mapping and credentials transform of Blakely within the security system of Mitchem with a motivation to enable tasks (clients) of Mitchem to access multiple separately authenticated resources with a single authentication (see Blakely, col. 1, lines 6-14).

As per claim 20, Mitchem teaches a system comprising (Figure 2 and associated text):

a first computer associated with a first requestor configured to generate resource requests (Figure 2, numeral element 20, col. 3, lines 10-16, discloses task 40 representing computational entities (first computer) which issues resource requests (col. 3, lines 20-22);

a second computer (figure 2, numeral element 10, col. 3, lines 17-19 disclose a security system including enforcement mechanism 20 and policy resolution 30 (second computer) including memory storing a resource data structure with resource nodes (col. 3, lines 39-42, policy resolution mechanism 30 maintains the set of security associations as an access matrix having tasks 40 and resources 25 as indices) each of which represents a respective resource and which has a respective resource identifier, a resource authorization parameter, and a resource authorization level (col. 3, lines 43-51, each entry of the access matrix defines a set of operations that a corresponding task 40 is permitted (i.e. resource authorization parameter and resource authorization level) to invoke on a particular resource 25 (i.e. resource identifier)), and the second computer configured to:

receive a resource request from a first requestor, the resource request including identifying information representing an operation to be performed with respect to a resource (col. 3, lines 23-27, enforcement mechanism 20 receives re resource request and identifies the requesting task 40, the requested resource 25 and the desired operation to be performed on the requested resource 25, col. 3, line 23-27);

map the resource request to a resource identifier (col. 3, lines 23-27, enforcement mechanism queries policy resolution by identifying requesting tasks 40, the requested resource 25 and the desired operation to be performed on the resource mapping the resource request to a resource identifier);

search the resource data structure for a resource node based on the resource identifier (col. 3, lines 44-45, policy resolution mechanism accesses a security database of the stored security association); and

determine whether the first requestor is authorized to perform the operation with respect to the resource based on the resource authorization parameter associated with the resource node (col. 3, lines 41-51, policy resolution mechanism 30 maintains the set of security associations as an access matrix having tasks 40 and resources 25 as indices and based on security association, policy resolution mechanism issues a response indicating whether the resource request is granted); and

a network over which the first and second computers communicate (col. 28-26, the security system 10 is distributed throughout a computing environment having a plurality of network computing machines, see also col. 3, lines 6-15).

Mitchem does not disclose but Blakely discloses a resource request including credentials (see abstract, see also col. 4, lines 50-65, col. 5, lines 7-21), translating the resource request to a resource inquiry request (col. 4, lines 23-30, Id mapping) to include the resource authorization parameter, the resource authorization parameter representing the permission necessary for a client to perform the operation (Id mapping is process of determining that client1 is mapped to ERID5 (resource authorization parameter representing the permission necessary for the client) and determining the resource request authorization based on whether the credentials in the resource request match the resource authorization parameter associated with the resource node (col. 4, lines 31-41, credential transform, where the mapped Id (if properly authorized) is used to access necessary credentials and the original client request is modified to incorporate the transformed credentials to access to the resource).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the Id mapping and credentials transform of Blakely within the access controlling method, system and computer executable instructions of Mitchem with a motivation to enable tasks (clients) of Mitchem to access multiple separately authenticated resources with a single authentication (see Blakely, col. 1, lines 6-14).

Claim 26 is a computer readable medium that stores computer executable instructions corresponding to the system claim 20. Claim 26 is rejected for the same reasons provided in the statement of rejection of claim 20 above (see Mitchem, claims 26 and 27, Blakely, claims 16-20)

As per claims 2, Mitchem teaches the method of claim 1 wherein searching includes searching resource nodes each of which represents a resource an includes a resource identifier (see Figure 2 and associated text, see col. 3, lines 41-45, an access matrix defining a set of operations that a corresponding task 40 is permitted to invoke on a particular resource 25 (nodes)).

As per claims 3, 13, 21, Mitchem teaches the method, the apparatus and the system according to claims 1, 12 and 20 respectively, wherein searching includes searching a directed graph structure and the resource data structure comprises a directed graph data structure (col. 2, lines 15, see also Figure 3 and associated text).

As per claims 4, 14 and 22, Mitchem as modified teaches the method, the apparatus and the system according to claims 1, 12 and 20 respectively, wherein

receiving a resource request (the credentials) includes receiving a digital certificate conforming to a simplified public key infrastructure (Blakely, col. 4, lines 55-57).

Therefore, it would have been to one of ordinary skill in the art at the time the invention was made to include the digital certificate taught by Blakely in the resource request of Mitchem to determine that the Mitchem's requester is authorized (and authentic) to access the security server before passing the requester identity to the policy resolution mechanism (Blakely, lines 58-62).

As per claims 9, 19 and 24, Mitchem as modified teaches delegating the credentials of a child node to a parent node in the resource data structure (Mitchem, col. 4, lines 31-37).

As per claim 11, Mitchem teaches the method of claim 1 wherein the resource request originates from a client computer directed to a server computer over a network (col. 3, lines 6-15, i.e. user applications accessing system resources such as network servers).

Claims 28 and 29 are computer executable instructions implementing the system of claims 22 and 24. Claims 28 and 29 are rejected for the same reasons provided in the statement of rejections of claims 22 and 24 above.

5. **Claims 5-8, 15-18, 23 and 27** are rejected under 35 U.S.C. 103(a) as being unpatentable over Mitchem and Blakely as applied to claims 1, 12 and 20 above, and further in view of prior art of record, U.S. Pat. No. 5,941,947 to Brown et al. (hereinafter "Brown).

As per claims 5-8, 15-18 and 23, Mitchem does not teach but Brown teaches the method, apparatus and the system according to claims 1, 12 and 20 respectively, wherein mapping includes mapping the resource request to the resource identifier and a resource authorization parameter (Brow, col. 14, lines 18-27) including an owner level authorizing complete access to the resource, an editor level authorizing read/write access to the resource and a reviewer level authorizing read only access to the resource and a none level denying all access to the resource (col. 17, lines 5-67).

Therefore, it would have been obvious to one of ordinary skill in the art at the tune the invention was made to modify the hierarchy of security servers server of Mitchem to that of Brown's Directory service to map the resource request to a resource identifier to flexibly manage user-specific access rights to different content entities when the number of subscribers (such as owners, editors, reviewers and guests) may be in the millions and the number of content entities may be in the tens of thousands, where these large quantities of access rights consumes large amounts of memory and often takes unacceptably long period of time to search (Brown, col. 1, line 38 through line 2, line 16).

Claim 27 is the article including instructions corresponding to claims 21 and 23. Claim 27 is rejected for the same reasons provided in the statement of rejections of claim 21 and 23 above.

6. **Claims 10, 25 and 30** are rejected under 35 U.S.C. 103(a) as being unpatentable over Mitchem and Blakely as applied to claims 9 and 20 and further in view of prior art of record, US Pat. No. 6,601,171 to Carter et al. (hereinafter " Carter")

Mitchem as modified doe not disclose but Carter discloses the method of claim 9 in which the resource request is handled based on the delegated credentials **(recited in claim 10)** (Carter, col. 1, line 34 through col. 2, line 16 discloses the key-oriented certificate (such as SDSl) used to delegate rights among entities of distributed computing systems (col. 1, lines 34-63)) and the delegation of credentials ((recited **in claim 25)** associated with the first requester (col. 1, line 60-63, Alice's key authorizes Bob's key (second requester) to use a service and Bob's key in turn authorizes Charlie's key (third requester) to use the service) to a second requester wherein the second requester can request resources using the credentials from the first requester as if it were the first requester (col. 2, lines 8-11, i.e. B (second requester) impersonates A (first requester)).

Therefore, it would have been obvious to one ordinary skill in the art at the time the invention was made to incorporate such delegation services into Mitchem's security system as modified to meet the urgent need in achieving seamless distribution of critical resources, and to make the power of computing resources available for more widespread use (Carter, col. 1, lines 23-34, see also col. l 3, lines 14-42).

Claim 30 is a computer readable medium that stores executable instructions corresponding to claim 25. Claim 30 is rejected for the same reasons provided in the statement of rejection of claim 25 above.

Conclusion

7. Prior arts made of record, not relied upon:

Structure for Decentralized Database Authorization, IBM Technical Disclosure Bulletin, vol. 22, Iss. No. 10, page 4692-4698, March 1980.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Taghi T. Arani whose telephone number is (571) 272-3787. The examiner can normally be reached on 8:00-5:30 Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Taghi T. Arani, Ph.D.
Examiner
Art Unit 2131
7/10/2005